Van Leeuwen & Van Leeuwen
Attorneys at Law
6123 Pebble Garden Court
Austin, Texas 78739
Phone # 512-301-6738
FAX # 512-301-6742

DATE: January 26, 2006

Number of Pages to Follow (including this cover sheet) 30

SEND TO:	United States Patent Office
Examiner:	**Son, Linh L D**
Group Art Unit:	**2135**
Tel No:	(571) 272-3856
Fax #:	571-273-8300

FROM:	Joseph T. Van Leeuwen **Van Leeuwen & Van Leeuwen** **Registered Patent Attorneys** 6123 Pebble Garden Court Austin, Texas 78739
Tel No:	512-301-6738
Fax No.	512-301-6742

Docket No. AUS920000264US1 **Serial No. 09/594,517** Atty: HR / JVL

Applicant: McBrearty, et al.

_X_ Transmittal Letter (2 copies)	_X_ Certificate of Facsimile (incl. w/Appeal Brief)
____ Amendment (___ pages)	____ Notice of Appeal
____ Amendment AF	_X_ Appeal Brief (27 pages)
____ Ext. of Time	____ Reply Brief
____ IDS Statement	____ Change of Address
____ Other	

Deposit Acct. No. 09-0447

Fees: Amendment _____ Notice of Appeal _____ Appeal Brief $500 Other _____

File: **0015**

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

IBM DOCKET NO. AUS920000264US1
DATE: January 26, 2006

Application Serial No.: 09/594,517

Sir:

Assignee Name: International Business Machines Corporation
Assignee Residence: Armonk, New York

Transmitted herewith for filing is the Patent Application of:

Inventors: McBrearty, et al.
For: System and Method for Securing Data on Private Networks

Enclosed are:

X Appeal Brief ($500).

Total: $ 500.00

X Please charge my Deposit Account No. 09-0447 in the amount of $500.00. A duplicate copy of this sheet is enclosed.

X The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 09-0447. A duplicate copy of this sheet is enclosed.

X Any additional filing fees required under 37 CFR Sect. 1.16.

X Any patent application processing fees under 37 CFR Sect. 1.17.

X No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and the undersigned hereby authorizes the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

By _____
Joseph T. Van Leeuwen, Reg. No. 44,383
Van Leeuwen & Van Leeuwen
Attorneys for Applicant
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

Atty Ref. No. 0015

RECEIVED
CENTRAL FAX CENTER
JAN 26 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
McBrearty, et. al.

Serial No.: 09/594,517

Filed: June 15, 2000

Title: System and Method for Securing Data on Private Networks

Group Art Unit: 2135

Examiner: Son, Linh L D

Attorney Docket No. AUS920000264US1

IBM Corporation
Intellectual Property Law Dept.
11400 Burnet Road
Austin, Texas 78758

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing or Transmission
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Joseph T. Van Leeuwen — 1/26/2006 (Date)

APPELLANTS' BRIEF

Sir:

A. INTRODUCTORY COMMENTS

This brief is filed in support of the previously filed Notice of Appeal, filed in this case on November 28, 2005, which appealed from the decision of the Examiner dated August 26, 2005 finally rejecting claims 1-5, 7-13, 15-21, and 23-27. Please charge the required fee under 37 CFR § 41.20(b)(2) to IBM Corporation Deposit Account No. 09-0447.

The two-month deadline for filing this Appeal Brief is January 30, 2006, therefore, no extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and the undersigned hereby authorizes the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

01/27/2006 TL0111 00000049 090447 09594517
01 FC:1402 500.00 DA

B. REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation, which is the assignee of the entire right, title, and interest in the above-identified patent application.

C. RELATED APPEALS AND INTERFERENCES

With respect to other prior or pending appeals, interferences, or judicial proceedings that are related to, will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such prior or pending appeals, interferences, or judicial proceeding known to Appellants, Appellants' legal representative, or assignee.

D. STATUS OF CLAIMS

1. Total number of claims in application

There are 24 claims pending. Three claims are independent claims (1, 11, and 19), and the remaining claims are dependent claims.

2. Status of all claims in application

- Claims canceled: 3 (claims 6, 14, and 22)
- Claims withdrawn from consideration but not canceled: None.
- Claims pending: 24 (1-5, 7-13, 15-21, and 23-27)
- Claims allowed: None
- Claims rejected: 1-5, 7-13, 15-21, and 23-27

3. Claims on appeal

The claims on appeal are: 1-5, 7-13, 15-21, and 23-27.

E. STATUS OF AMENDMENTS

All amendments have been entered in this case. No amendments have been made to the claims after the Final Office Action.

F. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide a concise summary of the claimed subject matter as follows. Claims 1, 11, 19, and 27 are independent claims. Note that claims 1-5, 7-10, and 27 are method claims, claims 11-13 and 15-18 are computer system claims, and claims 19-21 and 23-26 are computer program product claims. Independent claims 11 and 19 include means plus function limitations that correspond to the method steps set forth in independent claim 1. An information handling system capable of implementing Appellants' invention, as claimed in independent claim 11, is shown in Figure 7, and described in Appellants' specification on page 16, line 3 – page 17, line 17. Support for independent computer program product claim 19 is described in Appellants' specification on page 17, line 18 – page 18, line 5. In addition, support for each of the method steps and means plus function limitations of the independent claims are discussed below. The specific citations to Appellants' Figures and Specification are meant to be exemplary in nature, and do not limit the scope of the claims In particular, the citations below do not limit the scope of equivalents as provided under 35 U.S.C. § 112, sixth paragraph.

In one aspect of Appellants' invention, claims 1, 11, and 19 claim a method, computer system, and a computer program product for securely transmitting data in a network, the method comprising: sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers (see e.g., Figure 3, element 310; specification page 10, line 17 through page 11, line 18); receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data (see e.g., Figure 3, element 320; specification page 10, line 17 through page 11, line 18, and page 4, line 11 – page 4, line 17); establishing the secure connection between the first computer and the second computer (see e.g., Figure 2, elements 200 - 220; specification page 8, line 21 through page 10, line 16); transmitting a password across the secure connection, the password used to encrypt and decipher the data (see e.g., Figure 2, elements 225 - 235; specification page 8, line 21 through page 10, line 16);

encrypting the data using the password (see e.g., Figure 2, element 245; specification page 8, line 21 through page 10, line 16); and transmitting the encrypted data over a non-secure connection (see e.g., Figure 2, element 250; specification page 8, line 21 through page 10, line 16).

In another aspect, claim 27 claims a method for securely transmitting data between computers, the method comprising: establishing a secure connection between a first computer system and a second computer system, each of the computer systems connected to a computer network (see e.g., Figure 2, elements 200 - 220; specification page 8, line 21 through page 10, line 16); sending a password from the first computer system to the second computer system across the secure connection (see e.g., Figure 2, elements 225 - 235; specification page 8, line 21 through page 10, line 16); encrypting one or more packets of data using the password as an encryption key and responsively deciphering the data packets using the password as the encryption key (see e.g., Figure 2, elements 245 - 255; specification page 8, line 21 through page 10, line 16); transmitting the one or more packets of data from one of the computer systems to the other computer system (see e.g., Figure 2, element 250; specification page 8, line 21 through page 10, line 16); deciphering the one or more packets of data at the receiving computer system using the password as the encryption key (see e.g., Figure 2, element 255; specification page 8, line 21 through page 10, line 16); sending a request from the first computer system to the second computer system prior to the establishing of the secure connection (see e.g., Figure 2, elements 200 - 210; specification page 8, line 21 through page 10, line 16); and responding to the request by the second computer system (see e.g., Figure 2, elements 215 - 220; specification page 8, line 21 through page 10, line 16), the response further including: informing the first computer system that the second computer system accepts the data that is encrypted (see e.g., Figure 2, elements 215 - 220; specification page 8, line 21 through page 10, line 16 and page 4, line 11 – page 4, line 17).

Support for each of Appellants' means plus function limitations set forth in dependent claims is provided below. Note that general support for an information handling system and computer program product is discussed above. The specific citations to Appellant's Figures and Specification are meant to be exemplary in nature, and do not limit the scope of the claims, as provided under 35 U.S.C. § 112, sixth paragraph.

Claims 13 and 21 include the following means plus function limitation:

means for sending a second password, the second password replacing the password as the encryption key (see e.g., Figure 5, element 555; specification page 13, line 21 through page 14, line 29).

Claims 18 and 23 include the following means plus function limitations:

means for changing the password by including a counter as part of the password (see e.g., Figure 6, element 630; specification page 15, line 1 through page 16, line 2);

wherein the counter is incremented after each transmission between the first and second computer systems (see e.g., Figure 6, element 655; specification page 15, line 1 through page 16, line 2).

Claim 20 includes the following means plus function limitations:

means for transmitting the one or more packets of data from one of the computer systems to the other computer system (see e.g., Figure 2, element 250; specification page 8, line 21 through page 10, line 16); and

means for deciphering the one or more packets of data at the receiving computer system using the password as the encryption key (see e.g., Figure 2, element 255; specification page 8, line 21 through page 10, line 16).

Claim 25 includes the following means plus function limitations:

means for determining whether the data packets include sensitive information (see e.g., Figure 4, element 402; specification page 11, line 19 through page 13, line 20); and

means for selectively performing the encrypting based on the determination (see e.g., Figure 4, element 405; specification page 11, line 19 through page 13, line 20).

Claim 26 includes the following means plus function limitations:

means for analyzing the data packet and determining whether the data packet is encrypted (see e.g., Figure 4, element 422; specification page 11, line 19 through page 13, line 20); and

means for selectively deciphering the data packet based on the analysis (see e.g., Figure 4, elements 425-430; specification page 11, line 19 through page 13, line 20).

G. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 5, and 27 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over U.S. Patent No. 5,241,594 to Kenneth C. Kung (hereinafter "Kung") in view of U.S. Patent No. 6,539,479 to Thomas J. Wu (hereinafter "Wu"). Claims 2 and 3 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of U.S. Patent No. 6,317,829 to Paul C. Van Oorschot (hereinafter "Van Oorschot "). Claims 4 and 7 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of Japanese Patent No. 363039228A to Tachibana, Noriyuki (hereinafter "Tachibana"). Claims 8, 9, and 10 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of U.S. Patent No.4,249,180 to Eberle et al. (hereinafter "Eberle"). Claims 11, 12, 17, 19, 20, and 24 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of U.S. Patent No. 6,668,321 to Nendell et al. (hereinafter "Nendell"). Claims 13, 15, and 21 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of Nendell in further view of Van Oorschot. Claims 16, 18, and 23 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of Nendell in further view of Tachibana. Finally, claims 25 and 26 stand rejected under 35 U.S.C. § 103(a) as being obvious and therefore unpatentable over Kung in view of Wu in further view of Nendell in further view of Eberle.

H. ARGUMENTS – APPELLANTS' CLAIMS ARE NOT OBVIOUS, AND ARE THEREFORE PATENTABLE, OVER THE ART OF RECORD

I. Burden

The Office bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). As detailed below, the Examiner has failed to establish a *prima facie* case of obviousness.

2. References must teach or suggest all elements of the rejected claims

For an invention to be prima facie obvious, the prior art must teach or suggest all claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). As detailed below, the references cited by the Examiner do not teach or suggest all elements of Appellants' claims. Therefore, Appellants respectfully request that the Board reverse each of the Examiner's rejections.

a. Claims 1 5, and 27 – Kung in view of Wu

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 1, 5, and 27 over Kung in view of Wu.

Kung teaches a method of logging onto a remote "secure" computer from another "secure" workstation. Importantly, Kung does not teach or suggest sending passwords and data in anyway similar to that claimed by Appellants. Each of Appellants' independent claims are directed to securely transmitting data in a network with limitations that include:

- sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers;
- receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data;
- establishing the secure connection between the first computer and the second computer;
- transmitting a password across the secure connection, the password used to encrypt and decipher the data;
- encrypting the data using the password; and
- transmitting the encrypted data over a non-secure connection.

Contrary to Appellants' claimed limitations, Kung teaches that a user logs onto a first workstation (secure workstation 11) using a user ID and password. The workstation encrypts the

password supplied and compares the user ID and encrypted password with a stored encrypted password (stored in database 19a which is stored on workstation 11, col. 5, lines 50-53). If the encrypted password matches, the user is allowed access to secured workstation 11 (see Figure 4, and Kung's description at col. 5, line 37 to col. 6, line 2 and col. 6, lines 23-40). Kung further teaches that the user, once logged onto the secure workstation, can log onto a remote computer (remote computer 13).

Kung teaches a secure communication path that is established between the secure workstation and the remote computer and teaches that the user provides the remote computer with another user ID and another password. The remote computer uses a one-way encryption algorithm, substantially similar to that used by workstation 11, to encrypt the password and compare the supplied user ID and encrypted password to user IDs and encrypted passwords stored on the remote computer (in database 19b, see Figure 4, col. 5, line 37 – col. 6, line 50). Importantly, the password sent over Kung's secure path is not "used to encrypt and decipher ... data," as claimed by Appellants. Instead, Kung teaches that the password transmitted on a secure path is only used to log the user onto the remote computer (see col. 2, line 56 – col. 3, line 11). Kung never teaches or suggests using the password to encrypt or decipher data. Kung also fails to teach or suggest other limitations claimed in Appellants' independent claims. These shortcomings are detailed below.

First, Kung never teaches or suggests Appellants' claim limitation of "sending a request from a first computer to a second computer ***prior*** to establishing a secure connection, the first computer and the second computer included in a plurality of computers." Instead, Kung teaches that the secure workstation and the remote computer are in a distributed network where the computers are known to one another and that the network "***incorporates a secure communication path*** 20a as part of the network 20 that connects a secure user workstation 11 to the remote host computer 13." Nowhere does Kung teach or suggest that the either computer sends a request to the other "prior to establishing a secure connection," as claimed by Appellants.

Second, Kung never teaches or suggests "receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data," as claimed by Appellants. Instead, Kung's system relies on each system using a particular

one-way encryption algorithm to encrypt the passwords and also teaches that each computer is a "secured" computer that is interconnected to each other using a pre-established "secure communication path 20a." Kung never teaches or suggests one of the computers sending a message back to the other computer indicating that the computer accepts encrypted data.

Third, Appellants claim "establishing the secure connection between the first computer and the second computer." However, as explained above, the computers in Kung's network are always connected by a secure connection, and therefore, while Kung's computers ***use*** a secure connection supplied by the existing infrastructure (network 20), Kung does not teach or suggest ***establishing*** the secure connection between the two computers.

Fourth, Appellants claim "transmitting a password across the secure connection, the password used to encrypt and decipher the data." As described above, Kung does teach transmitting a user ID and password from the workstation to the remote computer so that a user of the workstation can log onto the remote computer. However, the password taught by Kung is ***never used*** "to encrypt and decipher" data, as claimed by Appellants. Instead, the password taught by Kung is simply used to authenticate the user on the remote computer system (see col. 2, line 56 – col. 3, line 11).

The Office Action admits that Kung does not teach "implementing the password transferred over the secured communication as the encrypt/decrypt keys." The Office Action also admits that Kung does not teach or suggest using the password to encrypt data. The Office Action further admits that Kung does not teach or suggest transmitting data, encrypted using the password, over a non-secure connection. Instead, contrary to Appellants' claimed invention, Kung teaches that the connection between the workstation and the remote computer is always secure and never teaches or suggests sending data over a non-secure network.

As illustrated above, while the Office Action contends that Kung teaches many of Appellants' claim limitation, a review of the reference reveals that Kung ***completely fails*** to teach or suggest ***any*** of Appellants' claimed limitations. Appellants respectfully submit that the Office Action misapplies the teachings of Kung to Appellants' claimed invention. To overcome the serious shortcomings of Kung, the Office Action alleges that Wu teaches these limitations.

As described below, Wu also falls far short of teaching or suggesting Appellants' claim limitations.

In each of Appellants' independent claims, Appellants claim certain limitations regarding the use of the password in encrypting/decrypting data. These limitations include:

- transmitting a password across the secure connection, the password used to encrypt and decipher the data;
- encrypting the data using the password; and
- transmitting the encrypted data over a non-secure connection.

The Office Action contends that Wu teaches these limitations. However, a review of Wu reveals that Wu neither teaches nor suggests these limitations. The Office Action cites Wu, col. 5, lines 45-53, and col. 6, lines 1-10 in support of this contention. These sections of Wu (from Wu's "Summary of the Invention") are reproduced below:

> SUMMARY OF THE INVENTION
>
> In summary, the present invention is a system and method for a server computer and a login procedure executed by a client host computer to establish a session key in a manner that is secure against both passive and active security attacks, and which utilizes the user's password so as to enable the server to determine whether or not the user in fact knows the password for the username account specified by the user during the login process.
>
> Prior to a login session, the server computer stores a password verification value x_p for each of a plurality of authorized users of the server computer. Each user generates a password verification value x_p by applying a first one-way hashing function to a password p specified by the user to generate a secret value x_s, and then applying a second one-way function to the secret value x_s to generate x_p.
>
> When a client computer attempts to establish a login session between the server computer and client computer, the following steps are performed. The server computer receives a user identifier from the client computer, and retrieves the password verification value stored by the server for the user. The client computer generates a first secret value w_s and then generates a corresponding first public value w_p by applying the second one-way function to the first secret value w_s. The client computer sends the first public value w_p to the server computer.
>
> The server computer generates a second secret value y_s and then generates a corresponding second public value y_p by applying the second one-way function to the second secret value y_s. The server computer sends the second public value y_p to the client computer. The server computer also generates a server session key K1 by applying a first predefined session key generation function to the first public value w_p, the retrieved password verification value x_p, and the second secret value y_s.

> The client computer regenerates the user's secret value x_S, and then generates a client session key K2 by applying a second predefined session key generation function to the second public value y_p, the first secret value w_S, and the regenerated secret value x_S.
>
> Then the client and server computers exchange a set of messages so that each can verify that the other computer's session key is equal to its locally generated session key. The login session is established only if the server computer verifies that the server and client session keys match.

Wu describes a login procedure that establishes a "session key" that is used in a public key/private key encryption protocol. Importantly, Wu never teaches or suggests encrypting ***any*** data with a password. Instead, Wu teaches that a one-way hashing algorithm is applied to a password to generate a "password verification value x_p." Wu then teaches using the password verification value along with a "first public [key] value w_p," and a "second secret value y_s," in order to generate a "server key K1" using a "predefined session key generation function." In addition to Wu's failure to teach or suggest encrypting data using the password, Wu also fails to teach or suggest using the password to generate the server key. Instead, Wu teaches first using a hash function with the password in order to generate a "password verification value" that is one of three inputs to the session key generation function.

In each of Appellants' Responses, Appellants have noted why the references cited in the Office Actions fail to teach or suggest Appellants' claimed invention. Wu never teaches or suggests encrypting ***anything*** with a password. Neither Kung nor Wu, alone or in combination with one another teach or suggest "*transmitting a password across the secure connection, the password used to encrypt and decipher the data; encrypting the data using the password; and transmitting the encrypted data over a non-secure connection,*" as claimed by Appellants in each of Appellants' independent claims.

In light of the fact that Kung in view of Wu, alone or in combination with one another, fail to teach or suggest Appellants' claimed limitations, Appellants respectfully request that the Board reverse the rejections of Appellants' claims 1, 5, and 27. Furthermore, as described in the sections below, the Examiner relied upon the combination of Kung in view of Wu in rejecting limitations included in each of Appellants' claims. Therefore, Appellants respectfully submit that each of Appellants' remaining claims is allowable over the art of record because Kung in

view of Wu simply does not teach or suggest Appellants' claim limitations included in each of these claims.

b. Claims 2 and 3 – Kung in view of Wu in further view Van Oorschot

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 2 and 3 over Kung in view of Wu in further view Van Oorschot. Claim 2 depends on claim 1 and adds the limitation of "automatically sending a second password based on an event, the second password replacing the password as the encryption key." Claim 3 depends on claim 2 and adds the limitation of "wherein the event includes a time interval event." Appellants respectfully submit that the keys taught by Van Oorschot. is not analogous to the passwords claimed by Appellants. Van Oorschot. is directed to a security system that uses "public keys cryptography" to "facilitate secure roaming of users." (see, Title, abstract). As described by Van Oorschot., and as known by those skilled in the art, public-key / private-key encryption is not analogous to encrypting data using a simple password, also called a "shared-key" system, as claimed by Appellants. Instead, in public-key / private-key encryption two keys are used – one to encrypt data and the other to decrypt the encrypted data. For encryption, the sender encrypts the data with the receivers "public key." This encrypted data can only be decrypted by the receiver using his or her "private-key." In contrast to Appellants' claimed invention, in public-key / private-key systems, as taught by Van Oorschot., the same key (or password) is never used to both encrypt and decrypt data. In Appellants' claimed invention, the same "password," and "second password," is used to both encrypt and decrypt data.

As described above, neither Van Oorschot, Kung, nor Wu,. taken alone or in combination with one another teach or suggest encrypting and decrypting data with a "password" that is updated with a "second password" that is also used to encrypt and decrypt data. Furthermore, claim 2 depends on claim 1 which is allowable over Kung in view of Wu for the reasons set forth in Section "a," above, and is therefore allowable for this reason as well. Likewise, claim 3 depends on claim 2 and is allowable because claim 1 is allowable as well as because, as described above, claim 2 is allowable. In light of these reasons, Appellants respectfully request that the Board reverse the Examiner's rejections of claims 2 and 3.

c. Claims 4 and 7 –Kung in view of Wu in view of Tachibana

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 4 and 7 over Kung in view of Wu in view of Tachibana. Claim 4 depends on claim 2 and adds the limitation of "wherein the event includes a preset number of transmissions occurring between two or more computers within the plurality of computers." Claim 4 depends on claim 1 and adds the limitations of:

- changing the password by including a counter as part of the password; and
- wherein the counter is incremented after each transmission between the first and second computer systems.

Tachibana is a single-paragraph Japanese patent "constitution" that fails to teach or suggest the limitations included in either claims 4 or 7. Regarding claim 4, Tachibana fails to teach or suggest an "event" that "includes a preset number of transmissions occurring between two or more computers within the plurality of computers." Instead Tachibana is directed at analyzing the timing between when a password was input by a user and when it was received – "[T]he reception input time interval is checked whether it is included in a registered input time interval permissible range. If so, an access to secret securing information is permitted: otherwise any access in inhibited." (see Tachibana's "Constitution," last two sentences) Tachibana does not teach or suggest an event used to change a password that is based on the number of transmissions between two computers. Tachibana also does not teach or suggest including "a counter" in the password or "incrementing" the counter after each transmission. Instead, as outlined above, Tachibana teaches including "timing" information so that the password is sent within a permissible time range and does not teach including counters in a password nor incrementing counters after each transmission.

As described above, neither Tachibana, Kung, nor Wu,. taken alone or in combination with one another teach or suggest the limitations set forth in claims 4 and 7. Furthermore, each of these claims depends on allowable claims as described in the preceding sections. In light of these reasons, Appellants respectfully request that the Board reverse the Examiner's rejections of claims 2 and 3.

d. Claims 8, 9, and 10 – Kung in view of Wu in further view of Eberle

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 8, 9, and 10 over Kung in view of Wu in further view of Eberle. Claim 8 depends on claim 1 and adds the limitation of "wherein the data is selectively encrypted." Claim 9 depends on claim 8 and adds the limitation of "wherein the selection is based on determining a sensitivity corresponding to the data." Finally, claim 10 depends on claim 8 and adds the limitations of:

- analyzing the data packet and determining whether the data packet is encrypted; and
- selectively deciphering the data packet based on the analyzing.

The Final Office Action admits that neither Kung nor Wu teach or suggest the limitations set forth in claims 8, 9, and 10, but contends that Eberle teaches each of these limitations. Eberle is a patent that was filed in 1978 and teaches a way of selectively encrypting individual characters before transmission over a modem. The user of Eberle's system surrounds text that he or she wishes to encrypted with control characters ("<" and ">"). Text that is not surrounded with such special characters is transmitted without encryption (see Fig. 10, col. 12, lines 34 – 59). While Appellants' claimed invention is focused on a password that is communicated between two devices, the cipher system of Eberle teaches away from transferring passwords. Instead, Eberle uses "cipher apparatus 10" that is a circuit used to encrypt/decrypt data. Because Eberle uses a hardware-based (fixed) encryption scheme, it will work "only if a terminal 12 that is used to communicate with a system 11 is equipped with an ***identical*** apparatus." (col 3, lines 45-56, emphasis added). Therefore, Eberle teaches away from transmitting a password from one system to another system and requires that the cipher apparatus in both systems be identical before any transmission. As Eberle was filed over 27 years ago, it is not surprising that Eberle teaches away from transmitting passwords used to encrypt/decrypt data.

Appellants respectfully submit that Eberle teaches away from being combined with Kung and Wu because of the fixed-nature of the cipher apparatus in Eberle that requires an "identical" apparatus in both systems with no suggestions whatsoever of updating the cipher apparatus (i.e., password) by transmitting the password from one device to another. Accordingly, Appellants

respectfully submit that the combination of Kung, Wu, and Eberle is improper as Eberle teaches away from transferring a password from one device to another. Moreover, each of these claims depends directly or indirectly on an allowable independent claim, as discussed in Section "a," above, and therefore these claims are also allowable for at least this reason. Consequently, Appellants respectfully request that the Board reverse the rejections of claims 9 and 10.

e. Claims 11, 12, 17, 19, 20, and 24 Kung in view of Wu in further view of Nendell

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 11, 12, 17, 19, 20, and 24 over Kung in view of Wu in further view of Nendell. Claim 11 is a computer system claim that includes substantially similar limitations as those of claim 1 as well as computer system component limitations as well as the limitation of a "means for deciphering the one or more encrypted packets of data at the receiving computer system using the password as the encryption key." Claim 12 depends on claim 11 and adds the limitation of "wherein the computer network is a private network." Claim 17 depends on claim 11 and ands the limitation of "wherein the computer network includes the Internet." Claim 19 is a computer program product claim that includes substantially similar limitations as those of claim 1. Claim 20 depends on claim 19 and includes the limitations of

- means for transmitting the one or more packets of data from one of the computer systems to the other computer system; and
- means for deciphering the one or more packets of data at the receiving computer system using the password as the encryption key.

Finally, claim 24 depends on claim 19 and includes the same limitation as claim 12 ("wherein the computer network is a private network"). While admitting that neither Kung nor Wu teach or suggest the limitations for these six claims, the Final Office Action contends that Nendell teaches these limitations, citing col. 3, lines 31-51 in support of this contention. This section of Nendell is reproduced below:

> In one implementation, a primary key is stored at a sending device and at a recipient device. The primary key and the other keys and passphrases can include a string of characters. The sending device generates a passphrase and an associated secondary key. The secondary key represents an encrypted form of the reconstruction capability of the passphrase that has been encrypted based on the contents of the primary key. The secondary key is transmitted from the sending

device to the recipient device when electronic communication is to be performed. The recipient device decrypts the secondary key using the primary key to reconstruct the passphrase. Reconstructing the passphrase can only be performed by recipient devices that possess the primary key. Accordingly, reconstruction of the passphrase demonstrates that the recipient device has received the secondary key and possesses the correct primary key. The passphrase can then be transmitted in return to the sending device or can be used locally at the recipient device to access documents that have been passphrase-protected or to access resources that are conventionally accessible by using passwords.

The Final Office Action summarizes the rejection of all of the limitations for all of these six claims as being that Nendell "teaches a method of transmitting a password from the first computer to the second computer to unprotect (decrypt the information)." Appellants respectfully disagree with the characterization of Appellants' claim limitations. Instead, Appellants' claim limitations are set forth in these six claims and include more than simply a "method of transmitting a password," as mischaracterized by the Examiner. Moreover, each of these claims include limitations (or depend on claims that include limitations) that were rejected as being obvious in light of Kung in view of Wu. As discussed in Section "a" above, Kung and Wu do not teach or suggest several of Appellants' limitations (specifically in claims 11 and 19), such as

- means for sending a request from the first computer system to the second computer system prior to establishing a secure connection, the first computer system and the second computer system included in a plurality of computer systems;
- means for receiving a response from the second computer system, the response indicating that the second computer system accepts packets of data that is encrypted;
- means for establishing the secure connection between a the first computer system and a the second computer system, each of the computer systems connected to a computer network;
- means for sending a password from the first computer system to the second computer system across the secure connection;
- means for encrypting one or more packets of data using the password as an encryption key;
- means for transmitting one or more of the encrypted packets of data from one of the computer systems to the other computer system; and

- means for deciphering the one or more encrypted packets of data at the receiving computer system using the password as the encryption key.

Rather than detailing why Kung in view of Wu in view of Nendell, alone or in combination with one another, do not teach or suggest any of these limitations, Appellants respectfully direct the Board to the discussion set forth in Section "a," above. The Examiner does not contend that Nendell teaches these limitations. Therefore, Appellants respectfully submit that each of these claims is allowable because they either include limitations, or depend on claims that include limitations, not taught or suggested by any of the references, either alone or in combination with one another. Accordingly, Appellants respectfully request that the Board reverse each of these rejections.

f. Claims 13, 15, and 21 – Kung in view of Wu in further view of Nendell in further view of Van Oorschot

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 13, 15, and 21 over Kung in view of Wu in further view of Nendell in further view of Van Oorschot. Claims 13 and 21 are each directed at sending a second password. This limitation is included in claim 2, the patentability of which was discussed in Section "b," above. In rejecting claims 13 and 21, the Examiner does not contend that Nendell teaches these limitations. Appellants hereby incorporate the arguments from Section "b," as such arguments also pertain to the patentability of claims 13 and 21.

Likewise, the limitation of claim 15 is substantially similar to the limitation of claim 3, the allowability of which having been previously argued in Section "b," above. Appellants also incorporate the arguments from Section "b," as such arguments also pertain to the patentability of claim 15. Consequently, neither Kung, nor Wu, nor Nendell, nor Van Oorschot, either alone or in combination with one another, teach or suggest the limitations of claims 13, 15, and 21, as discussed in Section "b," above. In addition, each of these claims depends, directly or indirectly, on an allowable base claim, as discussed in Section "a," above, and is therefore allowable for at least the same reasons as the base claim. Therefore, Appellants respectfully request that the Board reverse the Examiner's rejections of these claims.

g. ***Claims 16, 18, and 23 – Kung in view of Wu in further view of Nendell in further view of Tachibana***

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 16, 18, and 23 over Kung in view of Wu in further view of Nendell in further view of Tachibana. Claim 16 includes similar limitations as found in dependent claim 4 and is allowable for at least the same reasons as claim 4 is allowable, as discussed in Section "c," above. Likewise, claims 18 and 23 each include the same limitations as set forth in claim 7 and are therefore allowable for at least the same reasons as claim 7 is allowable, as discussed in Section "c," above.

Because neither Kung, nor Wu, nor Nendell, nor Tachibana, either alone or in combination with one another teach or suggest the limitations set forth in claims 16, 18, and 23, Appellants respectfully submit that each of these claims is allowable and respectfully request that the Board reverse the Examiner's rejections of these claims.

i. ***Claims 25 and 26 – Kung in view of Wu in further view of Nendell in further view of Eberle***

Appellants submit that the Examiner has failed to establish a prima facie case of obviousness in rejecting Appellants' claims 25 and 26 over Kung in view of Wu in further view of Nendell in further view of Eberle.

Claims 25 and 26 include substantially similar limitations as found in claims 8, 9, and 10, the allowability of which was discussed in Section "d," above. Because neither Kung, nor Wu, nor Nendell, nor Eberle, either alone or in combination with one another teach or suggest the limitations set forth in claims 16, 18, and 23, Appellants respectfully submit that each of these claims is allowable and respectfully request that the Board reverse the Examiner's rejections of claims 25 and 26.

Conclusion

For the foregoing reasons, Appellants submit that claims 1-5, 7-13, 15-21, and 23-27 are allowable over the art of record. Accordingly, Appellants respectfully request that the Examiner's rejections be reversed and claims 1-5, 7-13, 15-21, and 23-27 be allowed.

Respectfully submitted,

By _____

Joseph T. Van Leeuwen, Reg. No. 44,383
Van Leeuwen & Van Leeuwen
Attorneys for Appellants
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

I. APPENDIX OF CLAIMS

1. A method for securely transmitting data in a network, said method comprising:
sending a request from a first computer to a second computer prior to establishing a secure connection, the first computer and the second computer included in a plurality of computers;
receiving a response from the second computer, whereby the response informs the first computer that the second computer accepts encrypted data;
establishing the secure connection between the first computer and the second computer;
transmitting a password across the secure connection, the password used to encrypt and decipher the data;
encrypting the data using the password; and
transmitting the encrypted data over a non-secure connection.

2. The method as described in claim 1 further comprising:
automatically sending a second password based on an event, the second password replacing the password as the encryption key.

3. The method as described in claim 2 wherein the event includes a time interval event.

4. The method as described in claim 2 wherein the event includes a preset number of transmissions occurring between two or more computers within the plurality of computers.

5. The method as described in claim 1 wherein the network includes the Internet.

6. (canceled)

7. The method as described in claim 1 further comprising:
changing the password by including a counter as part of the password; and

wherein the counter is incremented after each transmission between the first and second computer systems.

8. The method as described in claim 1 wherein the data is selectively encrypted.

9. The method as described in claim 8 wherein the selection is based on determining a sensitivity corresponding to the data.

10. The method as described in claim 1 wherein the deciphering further comprises: analyzing the data packet and determining whether the data packet is encrypted; and selectively deciphering the data packet based on the analyzing.

11. A computer system comprising:
a networked computer system including a plurality of computers connected by a computer network, each of the computers including:
one or more processors;
a memory connected to the processors; and
a network connection that connects the computer with the computer network;
and
an encryption tool, the encryption tool including:
means for sending a request from the first computer system to the second computer system prior to establishing a secure connection, the first computer system and the second computer system included in a plurality of computer systems;
means for receiving a response from the second computer system, the response indicating that the second computer system accepts packets of data that is encrypted;
means for establishing the secure connection between a the first computer system and a the second computer system, each of the computer systems connected to a computer network;

means for sending a password from the first computer system to the second computer system across the secure connection;

means for encrypting one or more packets of data using the password as an encryption key;

means for transmitting one or more of the encrypted packets of data from one of the computer systems to the other computer system; and

means for deciphering the one or more encrypted packets of data at the receiving computer system using the password as the encryption key.

12. The computer system as described in claim 11 wherein the computer network is a private network.

13. The computer system as described in claim 11 wherein the encryption tool further includes:

means for sending a second password, the second password replacing the password as the encryption key.

14. (canceled)

15. The computer system as described in claim 11 wherein the means for sending is performed on a defined time interval.

16. The computer system as described in claim 11 wherein the means for sending is performed after a preset number of transmissions between the first and second computer systems.

17. The computer system as described in claim 11 wherein the computer network includes the Internet.

18. The computer system as described in claim 11 wherein the encryption tool further includes:

means for changing the password by including a counter as part of the password;

wherein the counter is incremented after each transmission between the first and second computer systems.

19. A computer program product in a computer usable medium for encrypting data between computers, said computer program product comprising:

means for sending a request from a first computer system to a second computer system prior to establishing a secure connection, the first computer system and the second computer system included in a plurality of computer systems;

means for receiving a response from the second computer system, whereby the response informs the first computer system that the second computer system accepts encrypted data;

means for establishing the secure connection between the first computer system and the second computer system, each of the computer systems connected to a computer network;

means for sending a password from the first computer system to the second computer system across the secure connection;

means for encrypting one or more packets of data using the password as an encryption key and means for deciphering the data packets using the password as the encryption key.

20. The computer program product as described in claim 19 further comprising:

means for transmitting the one or more packets of data from one of the computer systems to the other computer system; and

means for deciphering the one or more packets of data at the receiving computer system using the password as the encryption key.

21. The computer program product as described in claim 19 further comprising:

means for sending a second password, the second password replacing the password as the encryption key.

22. (canceled)

23. The computer program product as described in claim 19 further comprising:
means for changing the password by including a counter as part of the password, wherein the counter is incremented after each transmission between the first and second computer systems.

24. The computer program product as described in claim 19 wherein the computer network includes a private network.

25. The computer program product as described in claim 19 wherein the means for encrypting further comprises:
means for determining whether the data packets include sensitive information; and
means for selectively performing the encrypting based on the determination.

26. The computer program product as described in claim 19 wherein the means for deciphering further comprises:
means for analyzing the data packet and determining whether the data packet is encrypted; and
means for selectively deciphering the data packet based on the analysis.

27. A method for transmitting data securely between computers, said method comprising:
establishing a secure connection between a first computer system and a second computer system, each of the computer systems connected to a computer network;
sending a password from the first computer system to the second computer system across the secure connection;

encrypting one or more packets of data using the password as an encryption key and responsively deciphering the data packets using the password as the encryption key;

transmitting the one or more packets of data from one of the computer systems to the other computer system;

deciphering the one or more packets of data at the receiving computer system using the password as the encryption key;

sending a request from the first computer system to the second computer system prior to the establishing of the secure connection; and

responding to the request by the second computer system, the response further including:

informing the first computer system that the second computer system accepts the data that is encrypted.

J. EVIDENCE APPENDIX

Not applicable.

K. RELATED PROCEEDINGS APPENDIX

Not applicable.